INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Cost and Performance Analysis of Conceptual Design of Physical Protection Systems

B. DATE Report Downloaded From the Internet 8/13/98

Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #):
Sandia National Laboratories
M.J. Hicks (505) 844-7806
P.O. Box 5800
Albuquerque, NM 87185-0759

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: UM **Preparation Date:** 8/13/98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Cost and Performance Analysis of Conceptual Designs of Physical Protection Systems

M. J. Hicks, M. S. Snell, J. S. Sandoval, C. S. Potter
P. O. Box 5800
Sandia National Laboratories†
Albuquerque, NM 87185-0759
Phone (505) 844-7806 FAX (505) 844-0011 e-mail: mjhicks@sandia.gov

Abstract

CPA — Cost and Performance Analysis — is a methodology that joins Activity Based Cost estimation with performance-based analysis of physical protection systems. CPA offers system managers an approach that supports both tactical decision making and strategic planning. Current exploratory applications of the CPA methodology are addressing analysis of alternative conceptual designs. Hypothetical data is used to illustrate this process.

1 Introduction

Analysis of the cost and performance effectiveness of design alternatives is essential to a systems approach to physical security. While the concept of analysis of costs and performance is straightforward, implementation can be at the least tedious and, for complex designs and alternatives, can become nearly intractable without the help of structured analysis tools. CPA — Cost and Performance Analysis [1] — is a prototype integration of existing PC-based cost and performance analysis tools: ACEIT[1] (Automated Cost Estimating Integrated Tools) and ASSESS[2] (Analytic System and Software for Evaluating Safeguards and Security). ACEIT is an existing DoD (U. S. Department of Defense) PC-based tool that supports cost analysis over the full life-cycle of a system; that is, the cost to procure, operate, maintain and retire the system and all of its components. ASSESS is an existing DOE (U. S. Department of Energy) PC-based tool for probabilistic analysis of performance of physical protection systems designed for nuclear assets [2,3,4]. Two new tools are being developed: CATSS and PERFORM. CATSS (Cost Analysis Tool for Security Systems) [5] is being built around ACEIT. PERFORM, a performance data postprocessor, will integrate results generated by ASSESS and other performance analysis tools such as JTS (Joint Tactical Simulation). CPA is the over-arching architecture that aligns life-cycle costs with metrics of system and subsystem performance. The objective is to provide a tool that manages the life-cycle

---

† Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United Stated Department of Energy under Contract DE-AC04-94AL85000.

[1] ACEIT was developed by Tecolote Research, Inc. for the Electronic Systems Center, Cost Analysis Directorate, ESC/FM, Hanscom AFB, MA.

[2] ASSESS was developed for DOE by Lawrence Livermore National Laboratory and Sandia National Laboratories.

costs of security components and activities (Activity Based Costing), and then correlates costs with probabilistic metrics of performance in a format that facilitates both operational and strategic management decisions.

2 The CPA Architecture

The CPA architecture is illustrated in Figure 1. ASSESS is a path performance analysis tool. An icon of ASSESS is the Adversary Sequence Diagram (ASD), illustrated by ① in Figure 1 and shown in greater detail in Figure 2. An ASD models the areas of increasing protection of a physical security system separated or connected by path elements. The path elements function as either barriers (e.g., fences or surfaces) or as entry control points (e. g., gates or portals). Typically, there are multiple safeguards at each path element and those safeguards may be technological or procedural.

Within the CPA architecture, Figure 1, the structure of the physical protection system is extracted [②] from ASSESS [①] to launch the CATSS module [③]. This structure defines the first of three groups of cost objects [④]. Results are extracted from ASSESS for post-processing in the PERFORM module [⑤]. Cost and performance metrics can be offered at several levels: system, [⑥]and [⑦], subsystem, path element, and safeguards in both tabular, [④] and [⑧], and graphical formats, [⑨ and ⑩].

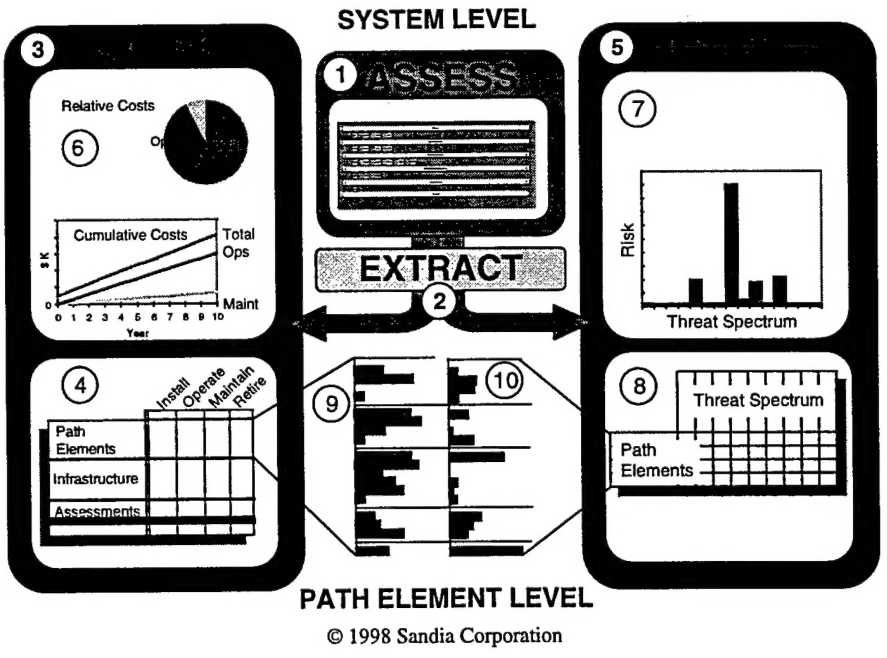


Figure 1. CPA Architecture

An ASD is a graphical representation of the physical security system.

Areas of physical protection are separated or connected by path elements.

Path elements function as
- barriers or
- entry control points.

Each path element has multiple safeguards, which may be
- technological
- procedural
- both.

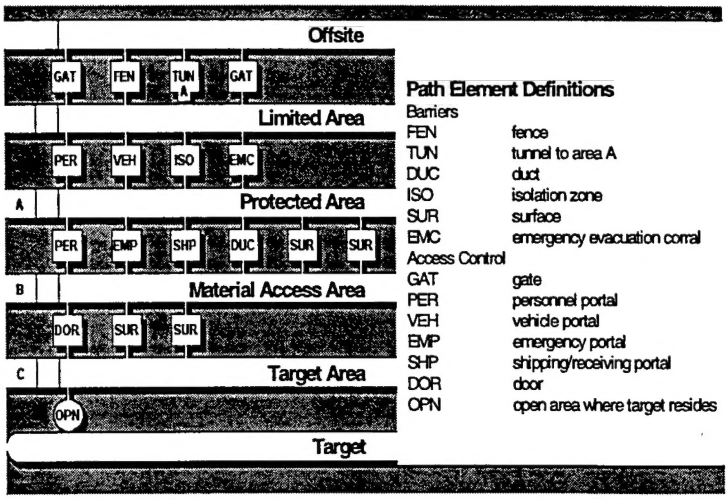


Figure 2. Adversary Sequence Diagram (ASD)

2.1 Cost Objects and Life-Cycle Phases of Physical Security Systems

In the CATSS module of CPA, cost objects of the physical security system are grouped into three broad categories: path elements, infrastructure and labor resources, and assessments. ACEIT is the data repository and the computational engine for CATSS. ACEIT supports a variety of economic analysis tasks, including management of funding categories, phased acquisitions, inflation, and cost in now- or then-year dollars. Costs are reported over the life-cycle phases: acquisition/installation, operations, maintenance and retirement or demolition/disposal as illustrated by the Summary Costs Spreadsheet ④ in Figure 1. Costs are allocated using the principles of Activity Based Costing (ABC) [6]. The five steps of ABC are: 1) identification of the cost objects; 2) identification of the processes and activities required to produce, operate, maintain or retire the cost objects; 3) identification of the materials and labor resources required to support the processes and activities; 4) assignment of resource costs to activities; and 5) assignment of activities to cost objects.

2.1.1 Cost Objects

2.1.1.1 Path elements

The listing of path elements and safeguards implemented is mapped from ASSESS to CATSS. This allows direct alignment of costs to performance at the path element level as illustrated by ⑨ and ⑩ in Figure 1.

2.1.1.2 Infrastructure

Infrastructure refers to all those cost objects of a physical security system that cannot be assigned to specific path elements. Consider the distinction between entry control and access control. Evaluation of a credential at an entry control point is a procedural safeguard executed at a path element. Access control is an infrastructure set of procedures that may use technology to generate the credentials at some central administrative facility.

Labor resources can be both cost objects themselves and resources assigned to cost objects. Within CPA, all labor resources are initially pooled under infrastructure. When members of a resource pool perform activities associated with security at specific path elements (cost objects) or other cost objects in the infrastructure, the costs of those resources are then assigned through the activities to the path element For example, a security inspector (SI) belongs to a labor resource pool. If that SI is posted at an entry control point, then the cost of the SI is mapped to the operational costs of the path element.

2.1.1.3 Assessments (or Evaluations)

Periodic internal and external assessments of the physical security system are so critical to confidence in the integrity of the system that CPA breaks them out as separate cost objects.

2.1.2 Life-cycle Phases

The cost estimation structure offered by the Summary Costs Spreadsheet provides a balanced approach to representing costs over the full life cycle of a system from installation through operations and maintenance to demolition and disposal, thus providing a context for capturing the full cost of ownership of the system.

2.2 Performance Metrics of Physical Protection Systems

Safeguards provide detection or delay. The safeguard performance metrics are threat- and tactic-specific. These safeguard metrics roll up to threat- and tactic-specific path-element performance metrics. A fundamental principle of physical protection is that systems must first detect an intrusion and then delay the intruder long enough to allow effective response. Effective response interrupts and successfully neutralizes the intruder before he can accomplish his objective. Therefore, the threat-specific systems-level performance metrics consider detection probabilities together with delay and response times.

2.2.1 Risk

A systems-level performance metric is risk, which is defined as follows.

$$\text{Risk} = P(A) \times [1 - P(E)] \times C \quad (1)$$

where, P(A), is Probability of Attack

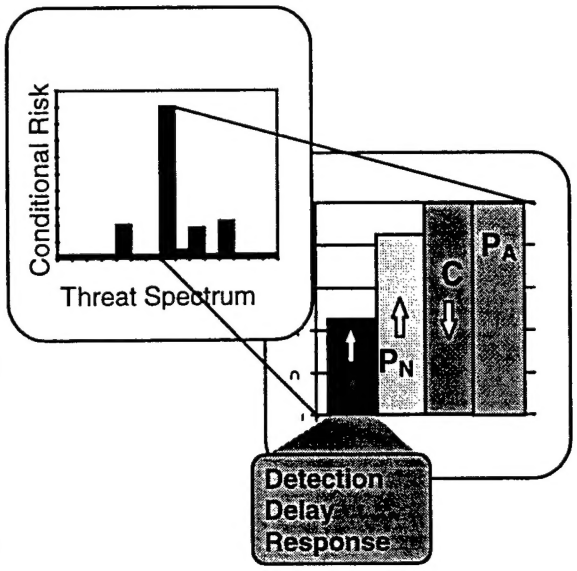
P(E), Probability of System Effectiveness, $= P(I) \times P(N)$, (2)

P(I) is Probability of Interruption,

P(N) is Probability of Neutralization,

C is Consequence.

If Probability of Attack is assumed to be one, then the performance metric is called conditional risk. Probability of Interruption is a function of the detection probabilities and delay times at the various path elements and of the time required for responders to interrupt the threat (response force time). The breakout of risk into its components is illustrated in Figure 3. Probability of Neutralization can be modeled in ASSESS and/or in JTS and should be verified with force-on-force engagement exercises. Similarly, response force times should be verified with limited-scope performance tests. Consequence may be defined by a normalized scale from zero to one or may be expressed in more absolute terms such as cost and time required to recover lost capabilities.



Risk should be reported across the threat spectrum for each target.

For each threat in the spectrum, conditional risk can be mitigated by:
increasing Probability of Interruption,
increasing Probability of Neutralization
and/or decreasing Consequence.

Probability of Interruption is a function of
detection,
delay and
response.

Figure 3. Breakout of Risk.

2.2.2 Detection and Delay

The PERFORM module of CPA offers decision makers systems level metrics of performance such as conditional risk across the threat spectrum, as illustrated by ⑦ in Figure 1. It allows analysts to drill down through path element and safeguard metrics of performance, ⑧ and ⑩ in Figure 1, to identify where and how technology can be used to improve performance or to control costs. The graphic illustrated by ⑩ in Figure 1 is demonstrated in Figure 4. The path elements shown in the ASD in Figure 2 are listed to the left. Path-element performance metrics (probability of detection and delay times) are shown for two modes of attack (on foot or in vehicles) and two threat tactics (force/stealth and deceit). From this figure analysts can readily examine system attributes and identify potential weaknesses. Long delays are desirable close to the target. Detection needs to occur, with high probability, before delay. Both detection and delay should be balanced. Referring to Figure 4 for the example facility, ❶ shows balanced but only moderate detection between the limited area and the protected area. ❷ shows both low and unbalanced detection. Minimum detection value at this layer is nearly zero. ❸ suggests a potential tradeoff between the requirements for security and those for safety at the emergency evacuation corral and at the emergency portal. ❹ shows balanced delay between the material access area and the vault interior.

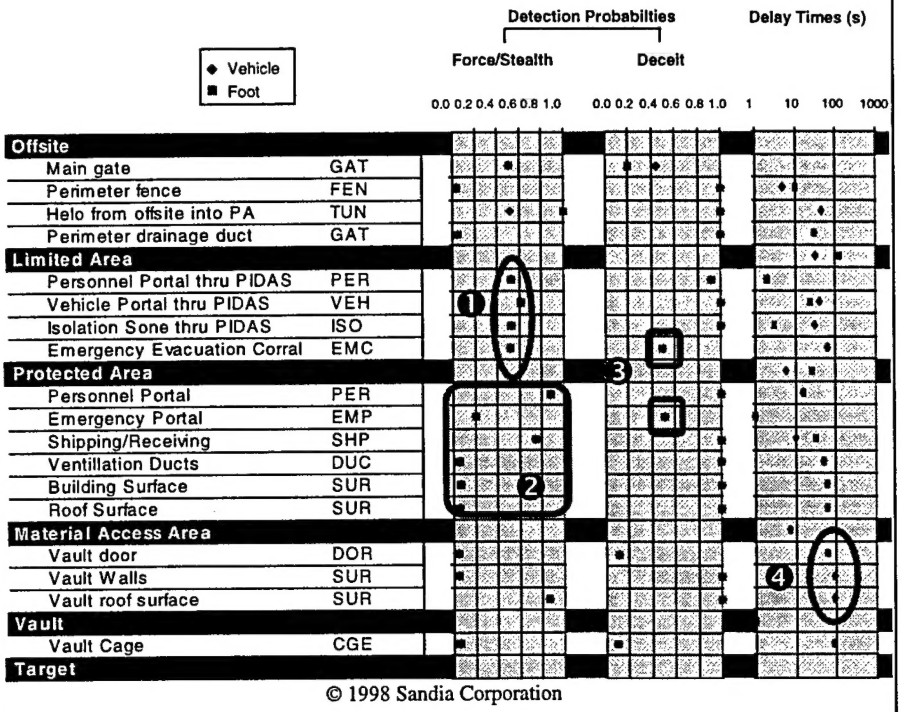


Figure 4 Metrics of path-element performance

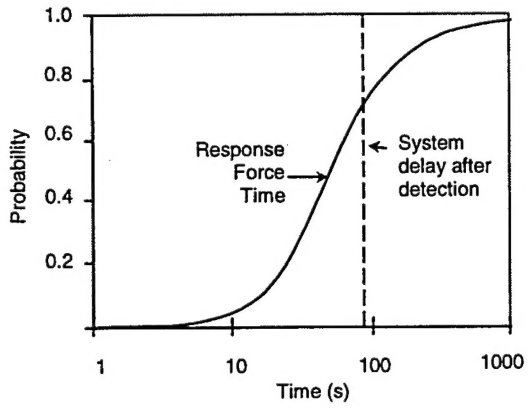
2.2.3 Response

The example in Figure 4 shows that Probability of Detection between the limited area and the protected area is 0.5, and zero (minimum value) between the protected area and the material access area. The adversary delay is about 0.7 s across the protected area, 0 s (minimum value) at the boundary between the protected area and the material access area, about 0.7 s across the material access area and about 70 s at the boundary between the material access area and the vault. The adversary task time at the target is about 80 s.

The relationship between delay after detection and response force time for this hypothetical example is shown in Figure 5. The distribution of response force times should be determined over all possible conditions.

The data in Figure 4 and Figure 5 suggest several issues in this hypothetical design that should be addressed. 1) While detection between the limited area and the protected area is balanced, is a value of 0.5 acceptable or does it need to be increased? 2) Detection between the protected area and the material access area should either be balanced or abandoned. Detection at this layer is of particular importance if there is more than one protected area within the limited area because detection at this layer provides threat location information to the response force. This argues for balancing the detection rather than abandoning it. This same argument holds for detection between the material access area and the vault. 3) Finally, delay needs to be balanced between the protected area and the material access area. Just how much detection and how much delay are required

depends on the protection objectives and the cost of improvements. To summarize, for the system as defined, a knowledgeable adversary would have a 0.5 probability of NOT being detected by this physical protection system. If detected, he has a 0.25 probability of being inside the vault before the response force arrives.



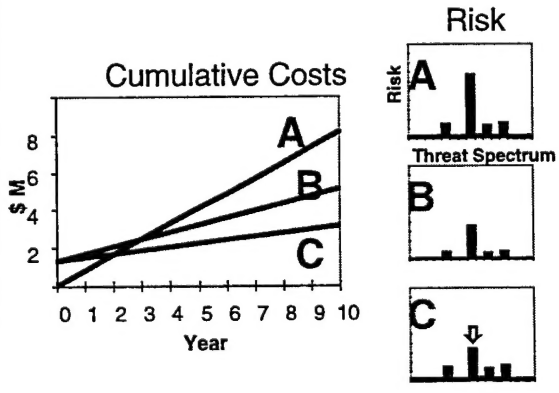
In this example, the minimum system delay for the adversary from detection at the protected area boundary to the vault cage is about 80 seconds.

25 % of the time the response arrives at the vault cage after the adversary.

Figure 5. Study of relationship between system delay and system response time

3 Cost and Performance analysis

As alternatives are identified that address the needs identified in the previous section, pertinent cost should be collected within the context of the cost estimation structure defined by the Summary Costs Spreadsheet. The costs and performance alternatives might be presented as illustrated in Figure 6. Of the three alternatives option C appears to be the best choice, provided the funds can be obtained for the initial $1.5 M installation investment. Option C would pay for itself in two years.



Option A: Do Nothing. Operations & maintenance costs accumulate at a rate of $800 K per year.

Option B Costs $1.5 M to install and $350 K per year to operate & maintain. Risk is reduced by a factor of 1.8 across the threat spectrum

Option C Costs $1.5 M to install and $200 K per year to operate & maintain. Risk is reduced by a factor of 1.8 for only one threat in the spectrum

Figure 6. Illustration of cumulative costs and associated risk profiles

4 Summary

This analysis has considered only the performance of a design, not the performance of a system as implemented. There are a number of other considerations that need to be addressed before risk can be estimated with confidence.

The CATSS module of CPA uses the principles of ABC to organize cost data by cost objects and life-cycle phases. ACEIT, the computational engine for CATSS, supports a variety of economic analysis tasks, including management of funding categories, phased acquisitions, inflation, and cost in now- or then-year dollars. The PERFORM module offers metrics of path element and safeguard performance from ASSESS analysis. It will address the integration of performance metrics from ASSESS with results from other performance analysis tools and limited-scope performance testing. The objective of CPA is to structure the collection and presentation of data in a manner that offers information in a compact form to both systems analysts and decision makers.

References

[1] M. J. Hicks, David Yates, William H. Jago, Alan W. Phillips, Dennis F. Togo, "Cost and Performance Analysis of Physical Security Systems," ADPA/NSIA 13th Annual Security Technology Symposium & Exhibition Government-Industry Exchange, June 9-12, 1997, Virginia Beach, VA.

[1] J. C. Matter, R. A. Al-Ayat & T. D. Cousins, "A Demonstration of ASSESS—Analytic System and Software for Evaluating Safeguards and Security," *Proceedings of the INMM 30th Annual Meeting,* Orlando, FL, July 1989.

[2] B. H. Gardner, Mark K. Snell & William K. Paulus, "Comparison of ASSESS Neutralization Module Results with Actual Small Force Engagement Outcomes," *Proceedings of the INMM 32nd Annual Meeting,* New Orleans, LA, July 1991.

[3] Byron H. Gardner, William K. Paulus & Mark K. Snell, "Determining System Effectiveness Against Outsiders Using ASSESS," *Proceedings of the INMM 32nd Annual Meeting,* New Orleans, LA, July 1991.

[4] David Yates, William H. Jago, Alan W. Phillips, *Cost Analysis Tool for Security Systems (CATSS), CR-0839*, Tecolote Research, Inc., 30 September 1996.

[5] Dr. Dennis Togo & Dr. Alistair Preston, "Activity-Based Cost Analysis of Security Services for a Nuclear Materials Site," prepared by Robert O. Anderson School and Graduate School of Management for Sandia National Laboratories under Contract No. DE-AC04-94AL85000, December 16, 1996.